IT Service Management (ITSM) Change Management Policy v1.0

Table of Contents

Objective **3**

Scope **3**

In scope: 3

Out of scope: 4

Policy Statements **4**

Roles and Responsibilities **8**

Exceptions **8**

Enforcement **9**

Approvals **9**

Version Control **9**

Glossary **10**

References **12**

Objective

The objective of this policy and the change management process is to control the lifecycle of all changes in the DMDC infrastructure. These policy statements have been established to protect the integrity of the DMDC infrastructure and associated outputs with the goal of achieving a highly resilient environment. Individuals who bypass the policies and processes for DMDC Change Management may put the DMDC at risk of business outage and non-compliance with government regulations, among other effects.

Scope

In scope:

This DMDC Change Management policy applies to employees, contractors, consultants, and other workers at the DMDC, including all personnel affiliated with third parties who have a need to implement a change to the DMDC infrastructure. This includes but is not limited to the following environments:

- Production (including 24x7)
- Sensitive Information Processing (SIPR) systems
- The Classified Data Center (CDC)
- Contractor Test (CT)
    - Demo1 and Demo2
- Disaster Recovery (DR)
- Stress Test region
- Quality Assurance (QA) region
    - Model1 and Model2
- DEV
    - Test1 and Test2
- Those workstations, laptops, printers and other DMDC standard devices that fall under the governance and overall control of the DMDC domain and Organization Unit (OU) standards for software and hardware.
    - For example: Global deployment of IE-10 and ‘Lockdown’ policies to all DMDC workstations would be applicable, whereas local break-fix issues or individual Commercial Off-the-Shelf (COTS) installations and modifications for a single workstation would be covered via Incident and Service Request tickets; Incident and Service Request procedures are outside the scope of this Change Management policy.

Out of scope:

The following areas are out of scope for this policy unless explicitly identified and shall be governed by the applicable policies for each:

- Development and lab environments not specifically referenced as being "In Scope" of this policy.
- Mainframe Platforms at the NPS (Naval Post graduate School)
- Service Request and Incident related activities for individual workstations, laptops, printers and other DMDC standard devices at the unit level (outside the scope of DMDC domain or Organizational Unit (OU) policy, patching requirements, etc.)
    - For example: Individual workstations and laptops used for general business purposes; workstations used for code generation, code testing or other individual purposes.

Policy Statements

Policy No.	Change Management Policy	Rationale
ChgM-1	Every change or modification to a DMDC managed computing environment is subject to the Change Management Policy and must follow the approved DMDC Change Management process and related procedures. Managed computing environments are delineated within the 'In Scope' section of this document.	Ensures the necessary visibility is provided for all changes and fundamentally this ensures consistency in process execution. Facilitates exchanging critical information related to real-time production activities.
ChgM-2	With the exception of an approved Emergency Change, no change can be made into any DMDC managed computing environment unless the change is first logged and officially approved in the designated DMDC change management / ITSM ticketing system. This policy statement applies to all changes made in DMDC managed computing environments, regardless of the type or category of the change.	This is a widely accepted and highly effective industry best practice, which is also supported through the NIST 800-53 v4 under Configuration Control and Control Objectives for Information and Related Technology (COBIT) v5 BAI06.01 through BAI06.04 This is essential for the management and recording of configuration changes and is critical for Incident Management teams who are responding to Major Incidents (aka: SRTs).

Policy No.	Change Management Policy	Rationale
ChgM-3	Any change that must be made immediately will be considered an Emergency Change. Generally, emergency changes are to restore a critical service during an outage situation and based on government priorities and direction. An Emergency Change must have a documented SRT number noted in the Emergency Change Request (ECR). In some situations an emergency change can be approved for very specific business-critical changes that are not related to an SRT or service restoration (e.g. proactive change to prevent an SRT or other service disruption); these changes must receive exception /authorization from the Division Director for that service or as appropriate from an Emergency Change Approver (ECA) and will only apply for that one specific change on that one date/time authorized.	Controlling and documenting emergency changes is a widely accepted and highly effective industry best practice which is also specifically called out as a control object in COBIT v5 BAI06.02
ChgM-4	Each CR that is submitted must have a complete and detailed Method of Procedure (MOP) document attached prior to submission for scheduling and approval. Every MOP must use the standardized MOP template which will include the business justification, detailed work instructions for the change, the verification plan, back-out plan, contact information, etc.	A detailed Method of Procedure (MOP) that will allow reviewers and approvers to understand the scope, complexity and ultimately the risks associated with the requested change. Depth and breadth of mandatory MOP details are commensurate with the complexity and overall risk profile identified within each CR.
ChgM-5	All non-emergency changes into production must be scheduled within an authorized Change Window. All approved changes must be completed within the Change Window approved for that specific change. These Change Windows are to be documented for each	The DMDC has a complex architecture with high-availability demands that cannot be compromised by change or releases that could ‘collide’ with one another and result in severe impact to the DMDC customer base or systems.

Policy No.	Change Management Policy	Rationale
	Service Environment. The Service Hours for each Environment are currently governed and coordinated via the Short Term Planning (STP) function. Change Requests must identify the Scheduled Start Date and approximate duration prior to implementation.	By viewing scheduled and approved changes for a specific day and time, the change management team has a higher probability of identifying where conflicts and collisions may occur and the incident management team can most effectively work to identify a potential cause of SRTs.
ChgM-6	All Requests for Change must be processed in a timely manner each business day. For this, every Division Approval group, Technical Review Board (TRB) and all Change Control Board (CCB) members must complete the review, risk assessment, and approval or rejection of all CRs assigned to that approval group each business day. At a minimum, TRB and CCB groups must process CRs in their queue twice each business day (morning and afternoon).	To ensure the efficient and timely execution of all changes, the responsible reviewers and approvers must make certain that all assigned requests for change are appropriately processed each day.
ChgM-7	DMDC Change Management Process Owner will ensure the change management policy and process is defined and published. The Change Management Process Manager will: 1. Ensure that the process, procedures and tools supporting this policy are documented and available, and that training is provided for all Change Management process participants and practitioners. 2. Provide reports that address the efficiency and effectiveness of the Change Management process.	The Process Owner is accountable to provide guidelines for how the Change Management process is to be performed and managed. Without an appointed Process Manager (ITIL defined and supported with a current RACI matrix), it is certain that the change process will not be properly sponsored and maintained.
ChgM-8	All Changes must be verified through review or testing before promotion into	Studies show that untested and unmanaged changes are often the cause of incidents and

Policy No.	Change Management Policy	Rationale
	Production is approved. The CR must include the necessary information to confirm and substantiate the review, or to confirm successful deployment in a Test and Pre-Production environment.	other issues that adversely impact service availability and the overall reliability of the production infrastructure. Ensuring that changes and releases are properly formed and tested not only increases the chances that issues will be identified before affecting production, it reduces the amount of productivity time lost when engineering teams are required to debug incidents and problems in production.
ChgM-9	The DMDC Information Assurance Branch (IAB) at its discretion may elect to review any and all Change Requests. The DMDC Change Management process manager will ensure that the designated IAB reviewers receive Change Request notifications from the ITSM tool.	The IAB Group is responsible for reviewing proposed changes to determine if the change will adversely modify the operational behavior of the configuration item (CI) and/or potentially violate the overall network and security policy. The IAB Group ensures that the change request follows the Security Technical Implementation Guides, DMDC Security policies, and that there is no potential loss of sensitive PII data. This review of the proposed configuration change can happen before or after the proposed change is tested
ChgM-10	Change requests must be submitted with sufficient lead time for each type of CR. The Change Management Process Manager will: 1. Provide an outline of the lead times and requirements for justifying the priority and urgency of any submitted change. 2. Document target resolution times for each authorized priority level within the Change Management process.	This is to ensure that the appropriate level of review and assessment of risk is performed, and that teams have adequate time to prepare for the change before the date of implementation.

Roles and Responsibilities

This policy calls for specific roles to be filled to ensure the effectiveness and efficiency of the Change Management process. The names of the DMDC personnel who will fill these roles will be documented and updated in the Change Management Process documentation and associated RACI matrix.

Role	Responsibility
Process Champion	The Process Champion is the business and operations interface and the person responsible for the official policy promulgation, promotion and encouragement to use the Change Management process throughout the DMDC Enterprise.
Process Sponsor	The role of the Process Sponsor is to support the Change Management policy by actively the related Change Management processes, ensuring support for the overall program and advising the IT organization on how to increase understanding and effective use of the Change Management process.
Process Owner	The Process Owner is accountable for the effectiveness of the process and efficiency of the supporting documentation for the process. This includes accountability for setting policies and providing leadership and direction for the development, design and integration of the process as it applies to other applicable frameworks and related ITSM processes being used and / or adopted for the DMDC. The Process Owner will be accountable for the overall health and success of the Change Management Process.
Process Manager	A role officially assigned to a single individual who will be accountable for all activities associated with the DMDC Change Management process. The Change Management process manager manages execution of the Change Management process and coordinates all activities required to process and manages changes. The Change Management process manager has the ultimate responsibility for the use of the Change Management process and procedures.
DMDC Leadership	It is the responsibility of all managers and leaders within the DMDC to ensure that all personnel subject to this policy are aware of this policy and are adequately trained to adhere to it.
DMDC employees and contractors	It is the responsibility of those DMDC employees and contractors who participate in the Change Management process to read, understand and work within the guidelines set forth in this policy and the related processes and procedures.

Exceptions

- Requests for exception to this policy must be submitted in writing to the Process Owner.
- Request exception will be reviewed by the Process Owner and must be further reviewed and approved by the DMDC Change Advisory Board (CAB).

Enforcement

Any violations of this policy will be reported to the appropriate member of management.

In the event that the DMDC Management believes a violation of this policy has occurred it shall notify the employee and/or vendor/supplier and provide a reasonable opportunity to address such circumstances as it believes constitute a violation of this policy.

Approvals

X

Kris Hoffman
Chief Information Officer

X

Wade Shaffer
Director, STS Division

Version Control

This DMDC Change Management Policy supersedes all existing Change Management policies or references to management of changes made in previously published DMDC Change Management, TRB-CCB or Configuration Management documentation.

Version	Date	Author	Change Description
1.0	22 Jan 2014	Corde Wagner	Final

Glossary

Term/Acronyms	Definition
Business Day	Generally Monday through Friday, 8 am to 5pm, for the organization implementing the change or providing support, not including approved holidays.
CCB (Change Control Board)	The role of the Change Control Board (CCB) is to provide a policy review of proposed changes to ensure that the proposed changes increase the operational efficiency of the DMDC IT Infrastructure in support of the mission of DMDC.
Change	The addition, modification or removal of anything identified as critical within the IT Configuration Baseline that could have an effect on IT Services. Note: For purposes of DMDC policy and the Change Management process, all synonyms for change also apply. They include but are not limited to: modify, adjust, deploy, release, configure, modification, manipulate, transform, correct, add, remove, delete, alter, switch, tweak, update, patch, upgrade, etc.
Change Advisory Board (CAB)	A group of people that support the assessment, prioritization, authorization and scheduling of changes. A change advisory board (CAB) is usually made up of representatives from: all areas within the IT service provider; the business; and third parties such as suppliers.
Change Type	**Normal:** A change that is not an emergency change or a standard change. Normal changes follow the defined steps of the change management process. **Standard Change:** A standard change is a change that could be made to a service or other configuration item for which the approach is pre-authorized by change management, and the standard change will follow an accepted and established procedure to provide a specific change requirement. By being “pre-authorized”, the implementer can be allowed to perform the pre-authorized change without being required to present the requested change to change management each time the change is to be implemented. Every standard change will have a change Method of Procedure (MOP) that defines the steps to follow, including how the change will be logged and managed as well as how it should be implemented. The MOP is part of what is reviewed by change management to arrive at the decision if the standard change will be pre-authorized for use. Example of a standard change: a password reset, provision of standard equipment, low risk database maintenance, etc. **Emergency:** A change that must be introduced as soon as possible. For example: ▪ To resolve a major incident that is impacting production services ▪ To implement a critical security patch in response to an active incident in the specified environment.
Change Request	CR: Change Request. Change Order ticket type within CA USD. (See Request for

Term/Acronyms	Definition
	Change (RFC))
Customer	Someone who receives goods or services from DMDC.
Change Windows	The defined period of time allowed for a change to be implemented. By best practices changes scheduled for a specific window of time must begin and end within that established change window. Examples of Change Windows for DMDC is the "Static Maintenance Window" which is an approved time for STS changes to be performed.
Emergency Change Approvers	The ECA is a designated approval authority and subgroup of the Change Advisory Board (CAB) that makes decisions about emergency changes.
ITSM	IT Service Management: The implementation and management of quality IT services that meet the needs of the business. IT service management is performed by IT service providers through an appropriate mix of people, process and information technology.
Outage	Outage: Where a service is not available, during it's agreed upon Service Availability, to many or all users. ▪ An unstable condition, as involving an impending abrupt or unexpected disruption to production and/or to business service(s). ▪ A stoppage in the functioning of a machine or mechanism due to a failure in the supply of power, electricity, data stream, etc.
Organizational Unit (OU)	A particularly useful type of directory object contained within domains is the organizational unit. Organizational units are Active Directory containers into which you can place users, groups, computers, and other organizational units. An organizational unit cannot contain objects from other domains.
Production	Production consists of all the assets and resources used to provide services to external and internal customers, including hardware, network, operating system software, COTS software, customer facing business applications software (e.g. owned by the DEERS, RAPIDS, DAP divisions, etc.), databases, and facilities (e.g. datacenter raised floors and other network/infrastructure rooms.)
Request for Change (RFC)	A formal proposal for a Change to be made. It includes details of the proposed change, and may be recorded on paper or electronically. The term is often misused to mean a change record, or the change itself.
Service	A means of delivering value to customers by facilitating outcomes customers want to achieve without ownership of specific costs and risks.
TRB (Technical Review Board)	In DMDC the role of the Technical Review Board (TRB) is to provide a technical review, assessment, classification, and approval of proposed changes into the DMDC production environments as made by the DMDC Enterprise. The TRB is responsible for evaluating proposed configuration changes based upon the

Term/Acronyms	Definition
	predetermined criteria associated with the CR requirements.
Vendor/ Supplier	A third party responsible for supplying goods or services that are required to deliver IT services. Examples of suppliers include contractors, commodity hardware and software vendors, network and telecom providers, and outsourced organizations (e.g. Managed Services Providers, etc.).

References

- DMDC Change Management TRB/CCB Procedure Document, v17, August 2013
- DMDC Change Request Guidebook, November 2013
- DMDC Emergency-Change_Guidebook, November 2013
- DMDC Change Management Method of Procedure Guidebook, December 2013
- Management of the Department of Defense Information Enterprise, DoD Directive 8000.1, February 2009
- Recommended Security Controls for Federal Information Systems and Organizations, NIST 800-53 rev-4, National Institute of Standards and Technology, US Department of Commerce, 4/30/2013
- ISO/IEC 20000-1:2011, Clause 5
- ISO/IEC 20000-2:2012, Clause 9
- COBIT v5 Enabling Processes, ISACA, 2012
- ITIL Service Strategy, v3, TSO, 2011
- ITIL Service Transition, v3, TSO, 2011
- ITIL Service Operation, v3, TSO, 2011
- The Visible Ops Handbook, IT Process Institute, 2010